GWDG

Self-Service PKI-Lösungen für eScience

von

Sebastian Rieger, GWDG
Jan Wiebelitz, RRZN

sebastian.rieger@gwdg.de
wiebelitz@rrzn.uni-hannover.de

R|R|Z|N
Universität Hannover

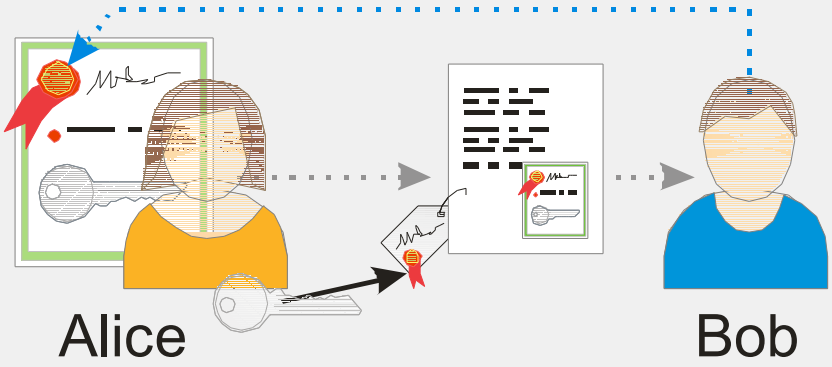
Gliederung

- Public Key Infrastruktur (PKI) Grundlagen
- PKI-Betriebserfahrungen in Göttingen und Hannover
- e-Science - Nutzung vom Zertifikaten in Grid-Umgebungen
- Self-Service Lösungen für PKI im e-Science Umfeld

X.509 Zertifikate als Basis für PKI

- Digitale Signatur: Absender verschlüsselt Hash mit privatem Schlüssel
- Identität des Absenders durch entschlüsseln mit öffentlichem Schlüssel verifizierbar
- öffentlicher Schlüssel ist signierter Bestandteil eines Zertifikats, durch vertrauenswürdige Zertifizierungsstelle
- z.B. bei S/MIME Signatur wird zusätzlich das Zertifikat hinzugefügt

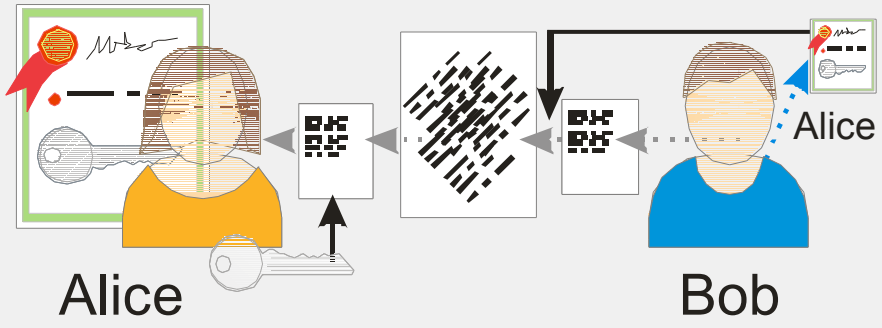
→ **Absender-Authentifizierung, digitale Identität**



X.509 Zertifikate als Basis für PKI

- asymmetrische Verschlüsselung: Absender verschlüsselt Nachricht mit öffentlichem Schlüssel des Adressaten (z.B. aus übermitteltem Zertifikat)
- Gültigkeit des öffentlichen Schlüssels mittels Verifizierung des Zertifikats
- nur Empfänger kann das Chiffrat mit seinem privatem Schlüssel entschlüsseln

→ **Empfänger-Authentifizierung**



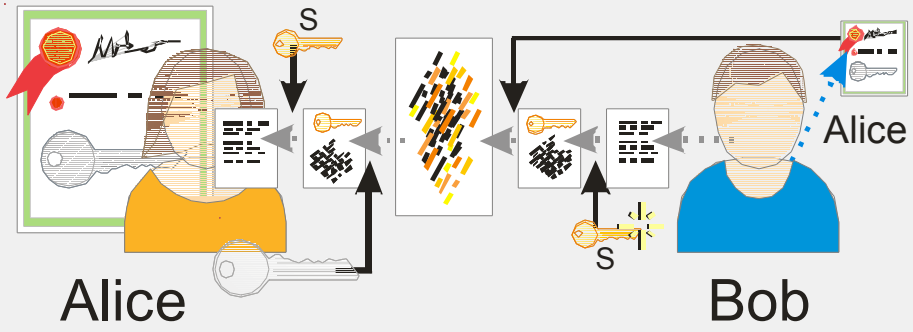
Einsatz von Zertifikaten

- asymmetrische Verschlüsselung wenig performant, mehrere Empfänger benötigen mehrere Chiffrate
- gängige Verfahren daher hybrid: vgl. SSL, TLS, S/MIME
- symmetrischer Sitzungsschlüssel für verschlüsselte Nachricht, wird asymmetrisch verschlüsselt ausgetauscht

→ **sicherer Schlüsselaustausch, hohe Performanz während der Sitzung**

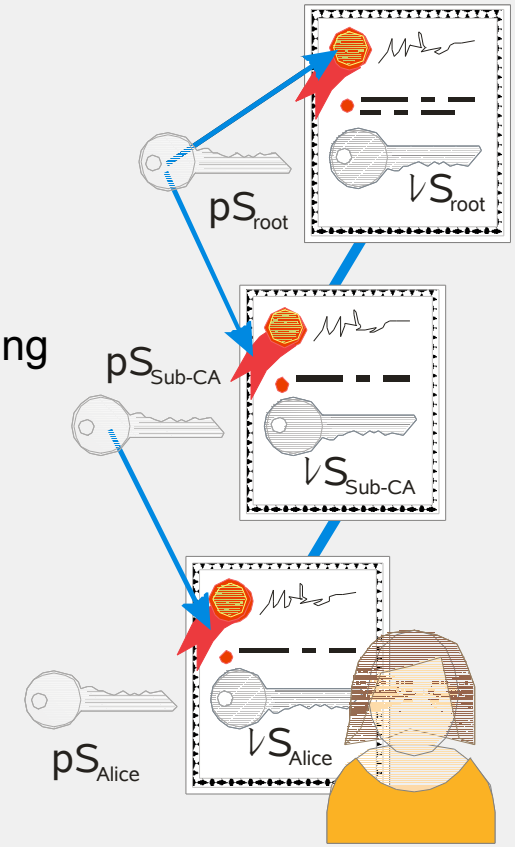
Einsatz von Zertifikaten im wissenschaftlichen Umfeld z.B. für:

- Server-Zertifikate (HTTPS, LDAPS, …), Client-Zertifikate (z.B. IPSEC)
- E-Mail und File Signatur sowie Verschlüsselung
- Code- und Objekt-Signatur



Aufgaben von Public Key Infrastrukturen

- Was ist eine PKI?
  - Struktur zum Verwalten und Nutzen von signierten öffentlichen Schlüsseln (Zertifikaten) asymmetrischer Schlüsselpaare.
  - Hierarchische Struktur unterschiedlicher Zuständigkeiten (Root-CA, Sub-CAs, RAs)
  - Festlegung von Richtlinien für Zertifikate (Identifizierung, Sperrung, private Schlüssel …)
  - Basis für Vertrauen in digitale Signaturen und Verschlüsselung



- Welche Funktionen erfüllt eine PKI?
  - Beantragen und Ausstellen von Zertifikaten
  - Prüfung und Zuordnung der Identität von Personen
  - Verwaltung und Verteilung der Zertifikate
  - Verlängerung und Sperrung von Zertifikaten

PKI an der Universität Hannover

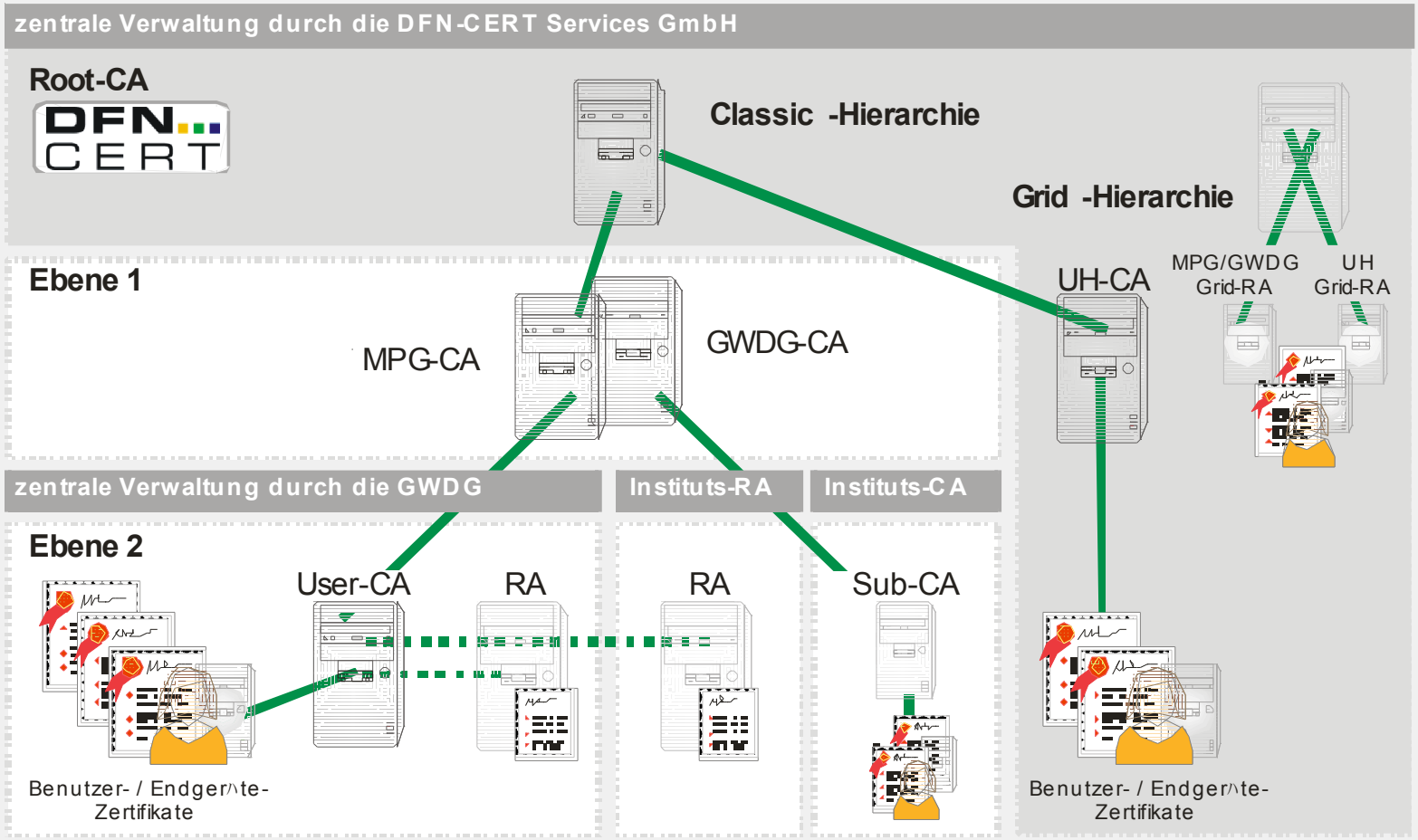
- Betrieb der CA an den DFN ausgelagert (DFN-PKI Dienst)
- Betrieb einer RA für die Universität Hannover
  - Nutzerregistrierung für die Universität Hannover
  - Beglaubigung von Anträgen für Server-Zertifikate
- Schwerpunkt Nutzerunterstützung
  - Public Relation (Vorträge, Workshops, ...)
  - umfangreiche Anleitungen
  - DFN-weiter Doku- und Infopool im Aufbau
- Betrieb einer RA für Grid-CA GridKA
  - Nutzerregistrierung für die Universität Hannover
  - Beglaubigung von Anträgen für Server-Zertifikaten

PKI der GWDG, MPG und Uni-Göttingen

- GWDG betreibt PKI für: Max-Planck-Gesellschaft und Georg-August-Universität Göttingen
  - Integration in „Classic“ und „Grid“ Hierarchie des DFN-Vereins
  - Institute können Zertifikate bei der User-CA (user-ca.mpg.de) GWDG (user-ca.gwdg.de) beziehen, Betrieb einer RA / CA an GWDG auslagern, oder selbst betreiben
  - Nutzerunterstützung, Workshops

- FAQs der Benutzer:
  - Muss ich dafür (wieder) nach Göttingen kommen? (persönliche Identifizierung)
  - Zertifikat erscheint nicht unter „Eigene Zertifikate“? (privater Schlüssel fehlt)
  - DFN-Zertifikat im Browser?

PKI in Göttingen und Hannover



e-Science - enhanced science

- neue Form des netzbasiertes wissenschaftliches Arbeiten
- Ziel ist es Forschungsprozesse zu erleichtern, verbessern und intensivieren
- vernetzter Nutzung von Ressourcen
- Aufbau einer Infrastruktur für das wissenschaftliche Arbeiten
  - Gigabit-Wissenschaftsnetzes des DFN
  - Grid Middleware Unicore und Unicore-Plus
  - Grid Community Centre Karlsruhe (GridKa)
- D-Grid Initiative
  - TextGrid (wissenschaftliche Textverarbeitung - Geisteswissenschaften)
  - C3-Grid (Klima)
  - HEP-Grid (Hochenergiephysik)
  - Medi-Grid (Medizin)
  - GACG (Astronomie)
  - InGrid (ingenieurwissenschaftliche Anwendungen)
  - DGI (Integrationsprojekt)

Grid-Computing

- Vision „Computerleistung aus der Steckdose“
- transparenter Zugriff auf Ressourcen (CPU, Storage, ...)
- effiziente Ressourcennutzung
- Arbeiten in Virtuellen Organisationen (VO)
  - Ressourcen und deren Benutzer sind Mitglieder einer VO
  - Mitgliedschaft unabhängig von irgendwelchen Grenzen
  - gemeinsames Ziel (Projekt, ...)
  - Voraussetzung: Zertifikat einer Grid-CA
- Grid-Middleware
  - UNICORE
  - auf Basis des Globus Toolkit (LCG, gLite)

PKI im eScience Umfeld

- Pro Land gibt es eine CA für Grid-Zertifikate
  - Zertifikate dieser CAs werden mit Grid-Middleware installiert
  - alle CAs zertifizieren nach PMA-konformen Policies
  - Middlewares auf Basis des Globus Toolkit benutzen diese Zertifikate
- Policy Management Authorities (PMA)
  - organisiert in der International Grid Trust Federation (IGTF)
  - weltweit drei PMAs
    - EUGridPMA für Europa
    - TAGPMA für Nord- und Südamerika
    - APGridPMA für den asiatisch-pazifischen Raum
  - nur akreditieren CAs werden in Grid-Middlewares akzeptiert
- Betrieb von regionalen RAs notwendig

Grid - Proxy Zertifikate I

- Problem:
  - Abbildung von Benutzer-Accounts durch Grid-Middlewares auf Pool-Accounts
  - Anwendungen sollen mit den Berechtigungen der Benutzer agieren
- Lösung:
  - Pool-Accounts nutzen Benutzer-Zertifikate
- nun zwei Probleme:
  - Privater Schlüssel des Benutzers muss ungesichtert der Grid-Middleware übergeben werden
  - Zertifikate tragen keine Berechtigung
- eine Lösung für beide Probleme:
  - Proxy-Zertifikate
    - kurze Gültigkeitsdauer
    - passender privater Schlüssel wird ungesichert an Grid-Middleware übertragen
    - Berechtigungen des Benutzers werden als Zertifikatserweiterung integriert

Grid - Proxy Zertifikate II

- Proxy-Zertifikate sind abgeleitete Zertifikate
  - Nutzer signiert sich Proxy-Zertifikate mit seinem privatem Schlüssel
  - DN des Benutzers erweitert um `CN=proxy`
  - kurze Gültigkeitsdauer (abhängig von Policy und Benutzung)
  - Benutzerattribute in Zertifikatserweiterung
  - „Chain of Trust“ vom Root-Zertifikat der CA über Benutzer-Zertifikat zum Proxy-Zertifikat
- Problem:
  - Benutzer-Zertifikat fehlt die Berechtigung zur Zertifizierung
    - `BasicConstraint: CA=false` oder fehlt
- Lösung:
  - RFC 3820 definiert kritische Zertifikatserweiterung `ProxyCertInfo`
  - aber wird aktuell nicht immer genutzt

Zusammenfassung Grid Computing

- Vision „Computerleistung aus der Steckdose“
- transparenter Zugriff auf verteilte Ressourcen
- Ressourcen und deren Benutzer sind Mitglieder in Virtuellen Organisationen
- Authentifizierung durch X.509-Zertifikate
- Nutzung von Proxy-Zertifikaten
- Delegierung von Rechten durch Zertifikatserweiterungen
- pro Land eine Grid-CA

Usability einer PKI im eScience…

- …“Muss ich dafür (wieder) nach Göttingen oder Hannover kommen?“
  - mobile Vergabe von Zertifikaten
    - z.B. vor Ort in Instituten oder auf Tagungen usw., ohne Wartezeit. Zertifikate mit begrenzter Gültigkeit (kürzer als Lebenszeit der Sperrliste) sind sofort verfügbar
  - Etablierung von Registrierungsstellen in den Instituten
    - schnelle Vergabe von Zertifikaten bzw. Identifizierung neuer Zertifikatnehmer vor Ort
  - eigenständige Verlängerung und Sperrung von Zertifikaten
    - durch den Besitzer bzw. Zertifikatnehmer
    - keine erneute persönliche Identifizierung – schlanker Beantragungsprozess
  - eigenständige Beantragung von zusätzlichen Zertifikaten
    - z.B. für Server, neue E-Mail-Adressen etc.
    - ohne erneute persönliche Identifizierung bei der Zertifizierungsstelle

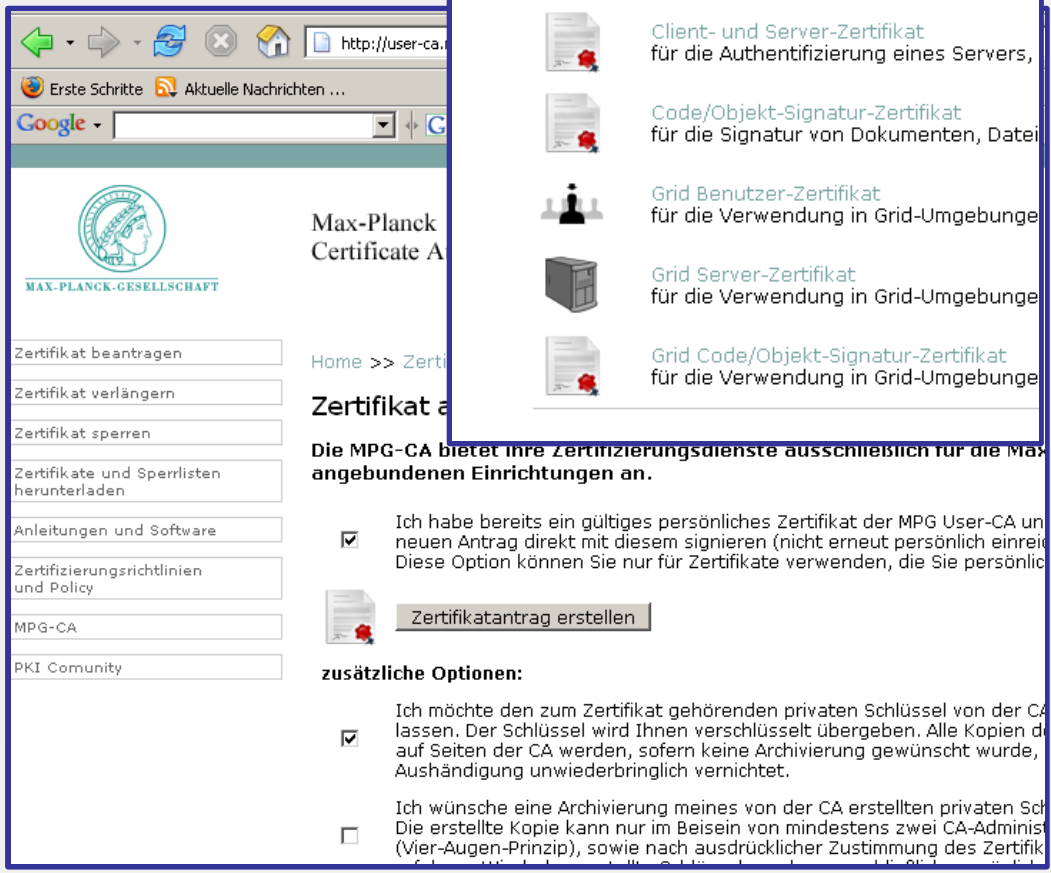
Anforderungen an die Zertifikat-Vergabe

- …“Warum erscheint mein Zertifikat nicht unter Eigene Zertifikate“?
  - Optionale Verteilung der Zertifikate inkl. privatem Schlüssel,
    - Vermeidung von Fehler bei der Verknüpfung von privatem Schlüssel und Zertifikat
    - Vereinfachung des Beantragungsvorgangs (…leider nur für den Zertifikatnehmer)
  - Optionale Archivierung der privaten Schlüssel
    - Reduzierung des Schadens bei versehentlicher Löschung des privaten Schlüssels
  - Unterstützung von Tokens (USB)
    - zur Speicherung privater Schlüssel und Zertifikate, um deren Sicherheit nachhaltig zu erhöhen.

- …“Warum ist das DFN Zertifikat nicht gleich in meinem Browser“?
  - automatische Verteilung der Zertifikate bzw. des Root-Zertifikats
    - Link und Anleitung auf HTTPS (Trust Center Zertifikat) Web-Seite, Kopieren des Mozilla / Firefox / Netscape Profils, OpenSSL certs, Active Directory

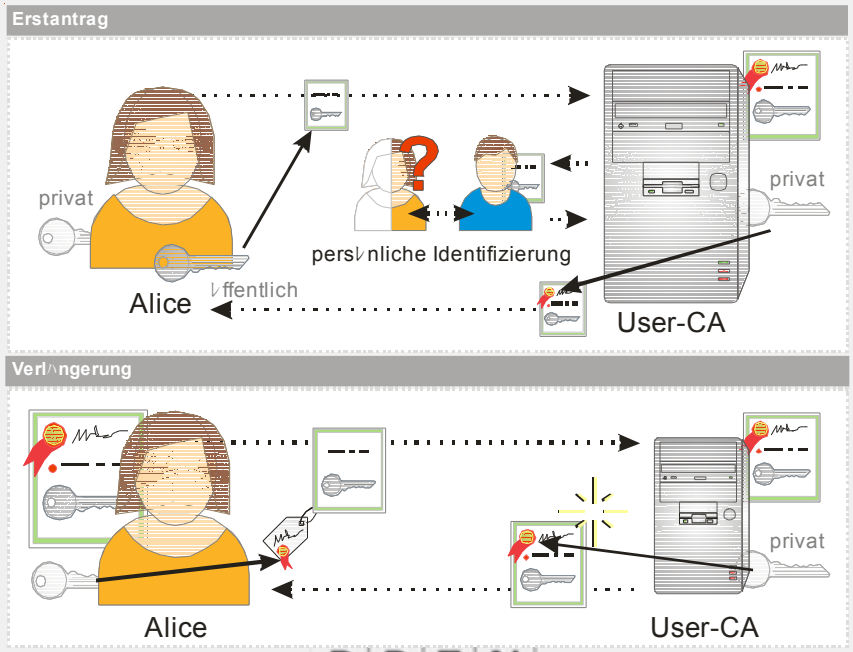
PKI im „Self-Service“

- zentrale Web-Schnittstelle für den Zugriff auf PKI-Leistungen
- Selbstbedienungsfunktionen für bestehende Zertifikatnehmer (basierend auf digitaler Signatur)
- ganzheitliche Lösung z.B. für Classic-, und Grid-Zertifikate
- Integration des kompletten Life-Cycles eines Zertifikats: Beantragung, Sperrung, Verlängerung
- Selbständige Beantragung weiterer Zertifikate



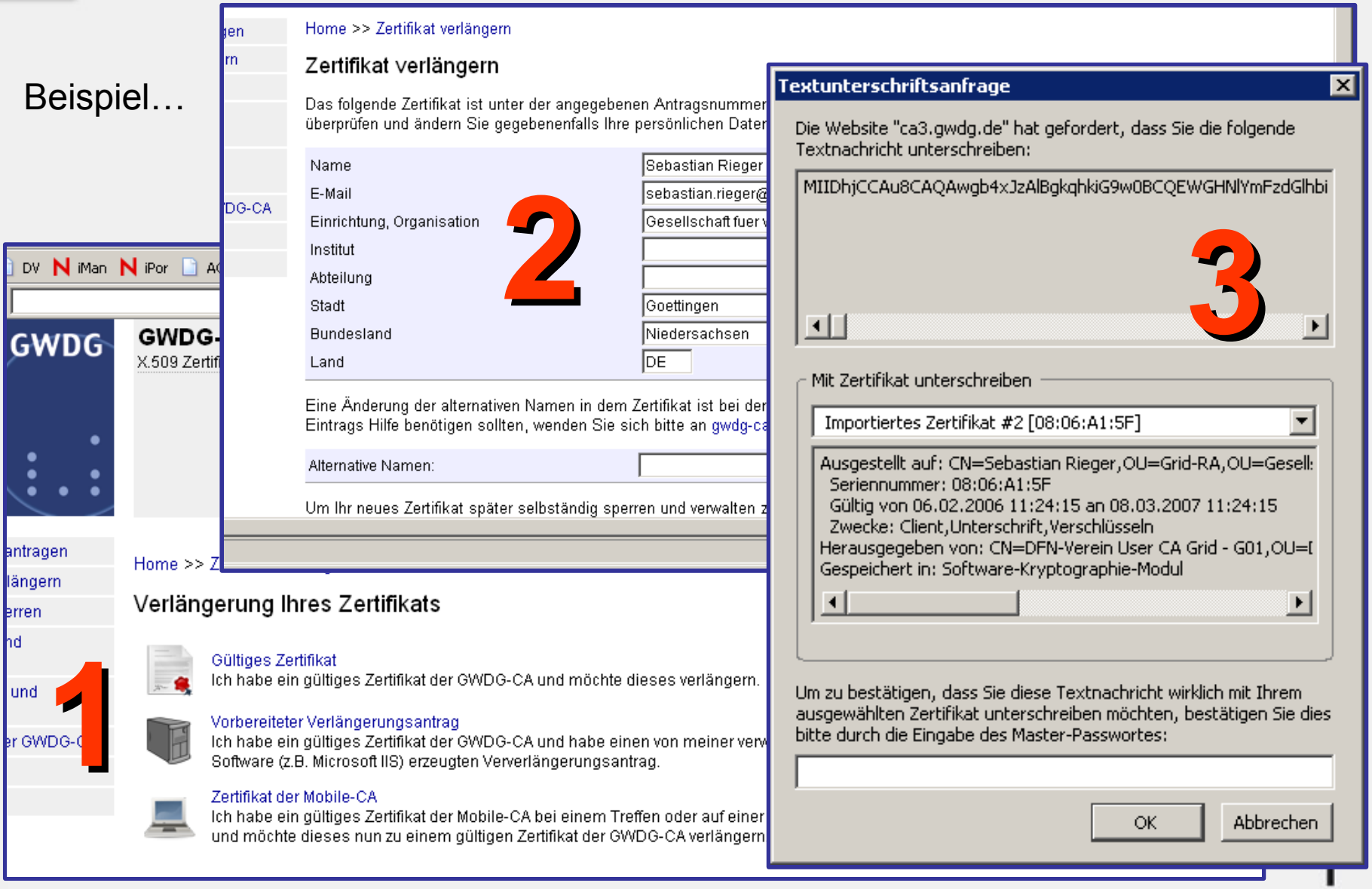
Verlängerung von Zertifikaten

- Zertifizierungs-Policy für Classic-Hierarchie gibt klare Regeln für Identifizierung von Zertifikatnehmern
- bei Erstantrag erfolgt persönliche Identifizierung
- für Verlängerung nicht erforderlich (digitale Signatur)
- Basis für Verlängerung i.d.R.: Re-Zertifizierung eines archivierten Zertifikatantrags (CSR)
- Funktioniert nicht mit Windows (bestehender privater Schlüssel wird nicht verknüpft)
- daher hier regulärer Neuantrag (xenroll mit altem Schlüsselpaar), Signatur mit CAPICOM
- Mozilla / Firefox / Netscape normal und window.crypto.signText()



Verlängerung von Zertifikaten

Beispiel…

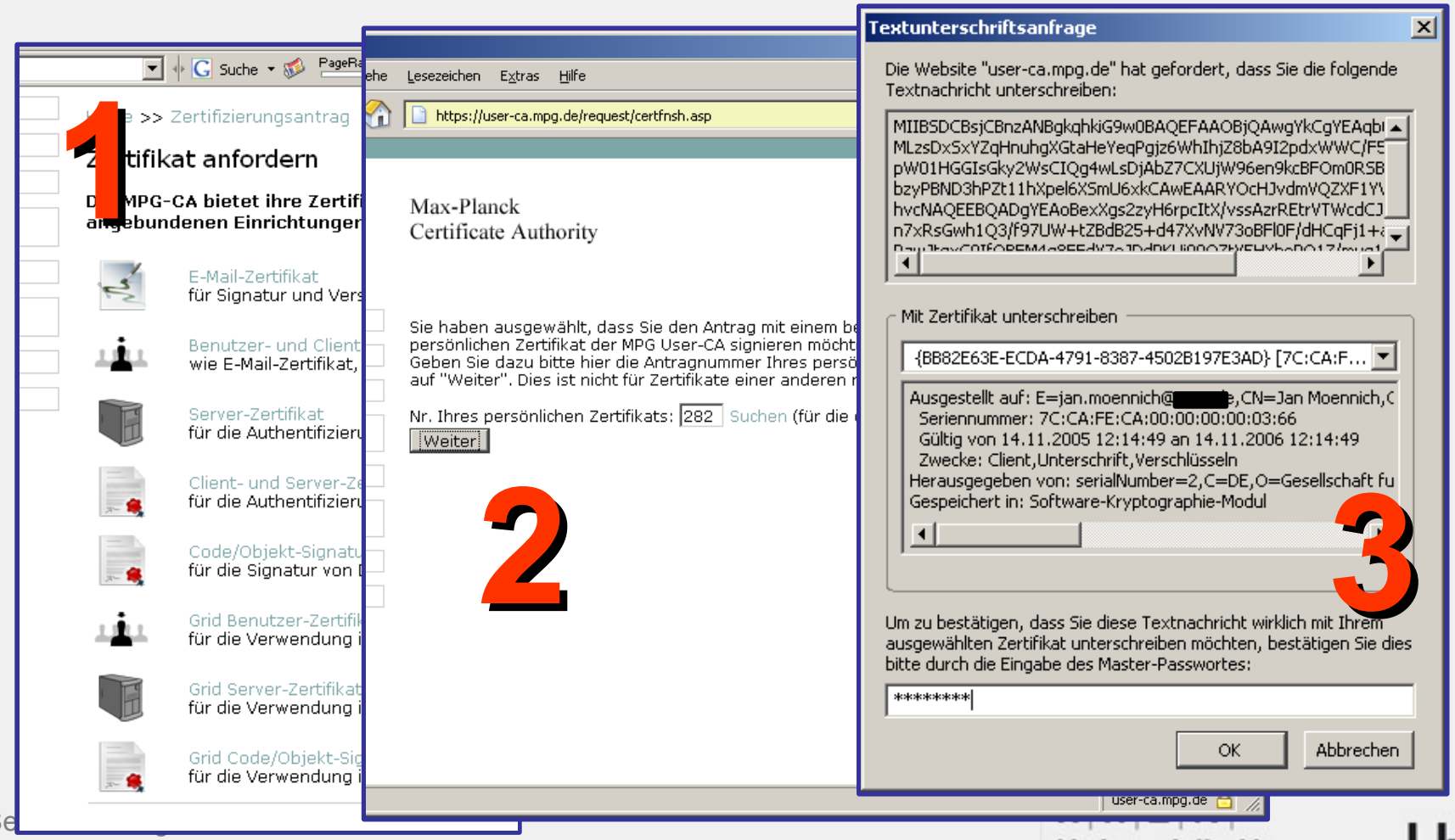


Zusätzliche Zertifikate beantragen

- Digitale Signatur der eingereichten CSRs für personalisierte RA Funktion verwendbar
- bestehender Zertifikatnehmer kann weitere Zertifikate ohne neue Prüfung bei CA einreichen
- z.B. kann ein Administrator weitere Server- / Client-Zertifikate, ohne erneute Identitätsprüfung beziehen
- Benutzer können z.B. neue E-Mail-Adressen beantragen (oder Ihren alternativen Namen im Zertifikat hinzufügen)
- Antrag geht direkt an die CA (entlastet ggf. RA), Signatur kann automatisiert geprüft und Zertifikat nach Bestätigung durch CA-Administratoren direkt ausgestellt werden
- Policy begrenzt dieses (sinnvollerweise!) ausschließlich auf Anträge der gleichen natürlichen Person
- für Anträge neuer Personen als Zertifikatnehmer somit persönliche Identifizierung z.B. durch RA erforderlich

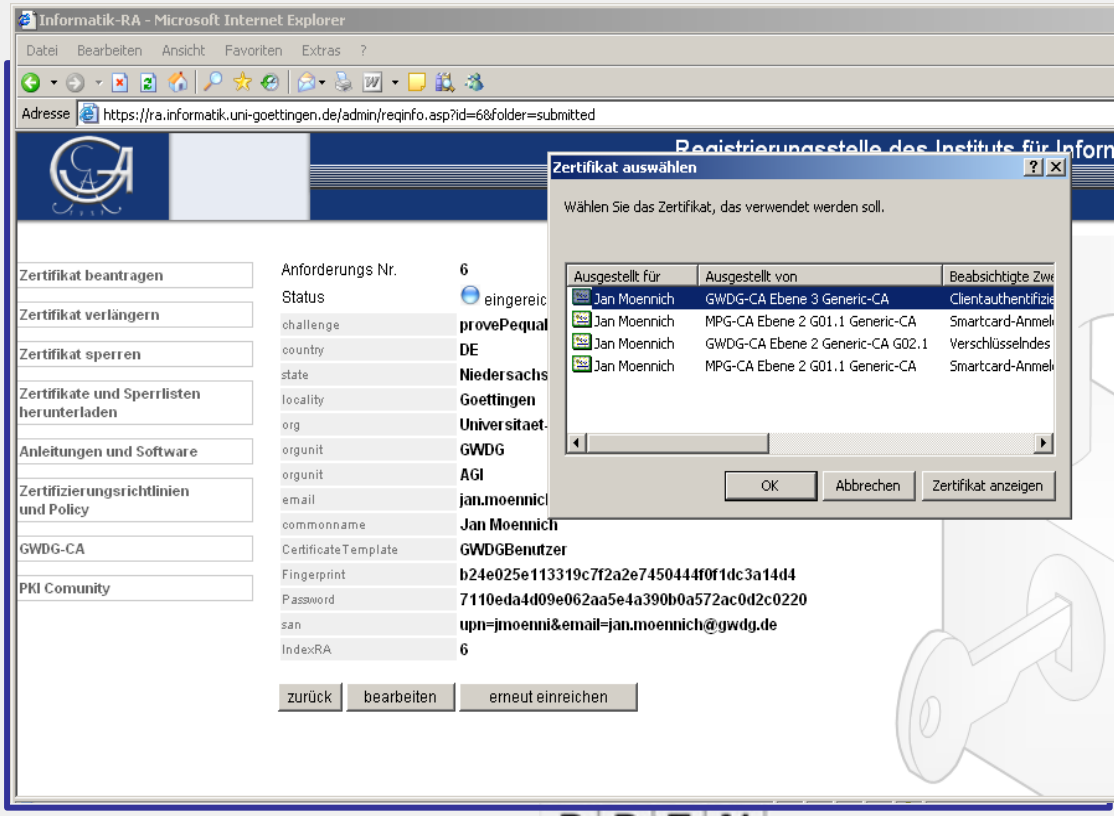
Zusätzliche Zertifikate beantragen

- Beispiel, Beantragung weiterer Server- / Client-Zertifikate für selben Administrator:



Etablierung von Registrierungsstellen (RAs)

- bestehende Zertifikatnehmer dürfen keine Zertifikate für neue Personen beantragen
- können aber mit wenig Aufwand RA werden, Policy erfordert zusätzlich: Akkreditierungsschreiben, RA-Teilnahme-Formular (Einhaltung CP / CPS)
- Hürde ist Betrieb der RA, kann analog zum Betriebsmodell des DFN, ausgelagert werden
- RA-Hosting hierbei individualisierbar (CI, Funktionalität)
- ausreichend große räumliche Verteilung senkt Kosten für die Identifizierung (für Zerfikatnehmer und -geber) Verzicht auf PostIdent



Schlüsselerzeugung und Archivierung

- in Classic-Hierarchie des DFN Schlüsselerzeugung durch CA zulässig, Schlüsselpaar muss nach Aushändigung auf Seiten der CA vernichtet werden (z.B. mehrfach mit randomisierten Daten überschrieben)
- Schlüsselarchivierung ist zulässig (nonRepudiation Flag darf nicht gesetzt werden), Zugriff nach Vier-Augen-Prinzip (vgl. geteiltes Archivar-Passwort) und Einwilligung des Zertifikatnehmers
- sofern Hardware-PSE / Token verwendet, so ggf. auch Unterstützung von Crypto-Appliances (freenigma) möglich, steigert Akzeptanz nachhaltig (wird derzeit geprüft)
- Policy erlaubt allerdings keine Schlüsselerzeugung für RAs
- Lösung über PIN-Briefe (nach Muster des DFN) möglich

derzeit realisierte Lösung:

- Anwender stellt Antrag ohne Schlüsselpaar bei CA / RA, fügt Passwort asymmetrisch verschlüsselt (öffentlicher Schlüssel von CA, Vier-Augen-Prinzip) hinzu
- CA entschlüsselt Passwort, setzt dies in PKCS#12 File, sendet dies an Zertifikatnehmer, optionale Archivierung des privaten Schlüssels (Vier-Augen-Prinzip), Archivar-Zertifikat

Fazit, Ausblick, PKI usability for eScience?

- aufgezeigte Lösungen adressieren Anforderungen der Zertifikatnehmer nach dezentraler bzw. nicht wiederholten Identifizierung und Vereinfachung der Schlüssel-Verwaltung
- Public Key Infrastrukturen haben nach wie vor „komplexen“ Ruf, häufig wird zu Gunsten unsicherer Lösungen (z.B. Passwörtern) auf Sie verzichtet
- sind aber Grundlagen für zukunftssicheres Identity Management und insbesondere dezentrale Grid-Anwendungen (vgl. Zuwachs von Grid-Zertifikaten)
- zukünftiges und gegenwärtiges Spannungsfeld: Security and Usability!
- Ziel sollte sein: Usability zu steigern ohne Security zu mindern
- möglich hierbei u.U.: skizzierte Self-Service Lösungen, Proxy-Zertifikate
- Ansätze wie automatische Zertifikatvergabe usw. lösen bestehende Probleme wie Phishing, Verlust der Authentizität, Verbindlichkeit, Integrität und Vertraulichkeit nicht!
- interessant auch: Lösungen für PKI Web-Services!, Barierrefreie PKI?

Vielen Dank für Ihre Aufmerksamkeit!
…haben Sie Fragen oder Anregungen?